UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

26 Andrews St., Dayton, OH 45410
including all outbuildings and curtilage

Case No. 3:23-mj-26

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHEMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. Sections 841 & 846; 843	Distribution of a controlled substance and conspiracy to commit the same; use of a communication facility to commit a felony

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sean C. Humphrey
Applicant's signature

Sean C. Humphrey, USPIS Task Force Officer
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone *(specify reliable electronic means)*.

Date: January 23, 2023

City and state: Dayton, OH

Caroline H. Gentry
United States Magistrate Judge

ATTACHMENT A

Property to be searched

The property to be searched, pictured below, is 26 Andrews St., Dayton, OH 45410, including all outbuildings and curtilage, further described as the right/west half of a duplex-style home with yellow siding and white trim. The number "26" is in white on the white pillar to the right of the front door.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 21 U.S.C. §§ 846, 843, and 841(a)(1), those violations involving unknown suspects and occurring after January 1, 2023, including:

a. Log books, records, payment receipts, notes, and/or customer lists, ledgers, telephone numbers and other papers or electronic records relating to the transportation, ordering, purchasing, processing, and distribution of controlled substances, including information reflecting transactions for the purchase/sale of narcotics.

b. Papers, tickets, notices, credit card receipts, wire transfer receipts, travel schedules, travel receipts, passports, and/or records, and other items relating to domestic and foreign travel to obtain and distribute narcotics and narcotics proceeds, including, but not limited to airline receipts, vehicle rental receipts, credit card receipts, travel schedules, diaries, hotel receipts, truck logs, travel agency vouchers, notes, records of long distance telephone calls, e-mail, calendars and other correspondence.

c. Address and/or telephone books and papers reflecting names, e-mail and physical addresses and/or telephone numbers of individuals, partnerships, or corporations involved in drug trafficking and money laundering.

d. Financial records, financial statements, receipts, statements of accounts and related bank records, money, drafts, letters of credit, money orders and cashier's checks receipts, passbooks, bank checks, escrow documents, and other items evidencing the obtaining, secreting, transfer, and/or concealment of assets and the obtaining, secreting, transferring, concealment, and/or expenditure of money.

e. Electronic equipment such as pagers, computers, Computer systems, cell phones, PDA devices including hardware, software, data contained in the main unit, printers, external modems, monitors, fax machines and/or other external attachments, electronic organizers, facsimile machines, cellular telephones, caller ID, telephone answering machines, police scanners and two-way radios.

f. United States currency, precious metals, coins, bullion, jewelry, and financial instruments, including, but not limited to stocks and bonds.

g. Photographs and/or photographic albums or video tapes and recordings of houses and other real estate, automobiles, and of other assets, persons, and/or controlled substances.

h. Indicia of occupancy, residency, and/or ownership of the premises and vehicles including, but not limited to utility and telephone bills, canceled envelopes, keys, deeds, tax bills, titles, and vehicle registrations.

i. Contraband, such as controlled substances and other materials, paraphernalia and/or equipment and tools used in the drug trade.

j. Firearms or ammunition.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

ATTACHMENT C

Upon delivery of the SUBJECT PACKAGE (as described in the Affidavit submitted with the warrant application) and the SUBJECT PACKAGE taken into the residence at the PREMISES, the search warrant will be executed at the PREMISES. The search warrant will be executed at the PREMISES if, and only if, the SUBJECT PACKAGE is taken into the residence located at the PREMISES.

Furthermore, if the SUBJECT PACKAGE is transferred to any vehicle or other property located within this Court's jurisdiction, this warrant authorizes law enforcement to secure the location until an application for a new warrant can be obtained.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF 26 ANDREWS ST, DAYTON, OH 45410	Case No. 3:23-mj-26 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR AN ANTICIPATORY WARRANT TO SEARCH AND SEIZE

I, Sean C. Humphrey, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for an anticipatory warrant to search the premises known as 26 Andrews St. Dayton, OH 45410, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B. Based on my training and experience, I submit that, if the relevant condition in Attachment C is satisfied, there will be probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and property designed for use, intended for use, or used in committing a crime—namely, drug trafficking and conspiracy to commit drug trafficking, in violation of Title 21 U.S.C. §§ 841 and 846; and use of a communication facility to commit a felony, in violation of Title 21 U.S.C. § 843—exists and will be found at the PREMISES.

2. I am employed by the Dayton Police Department and have been so since July of 2008. I have been assigned to Patrol Operations and am currently assigned to the Narcotics Bureau

- Montgomery County Regional Agencies Narcotics and Gun Enforcement (RANGE) Task Force. I have extensive prior experience in investigating drug cases that resulted in successful prosecution of persons involved in trafficking of drugs, possession of drugs and other related offenses. I have been involved in narcotics related arrests, executed search warrants that resulted in the seizure of narcotics and participated in undercover narcotics purchases. Through training and experience, I am familiar with the manner in which persons involved in the illicit distribution and sales of controlled substances often operate. These subjects usually attempt to conceal their identities, as well as the locations at which they reside and where they store controlled substances and the illegal proceeds derived there from. Through training and experience, I am familiar with the practices of narcotics distributors and sellers, whereby they attempt to conceal the true nature, source and location of proceeds of illegal activity, commonly referred to as money laundering. I have been a Task Force Officer with the United States Postal Inspection Service since November 2022. I am presently assigned to the Cincinnati Field Office of the United States Postal Inspection Service, Pittsburgh Division, with investigative responsibility for Southern District of Ohio. Part of my responsibility involves investigating the illicit use of the United States Mails in the transportation of narcotics, other dangerous controlled substances, and financial proceeds from, or instrumentalities used in, the sale of such narcotics and controlled substances (hereinafter, "Drugs and/or Proceeds").

3. Based on my training and experience, I have become aware that drug traffickers frequently use Priority Mail Express, a business-oriented overnight service offered by the United States Postal Service, to transport narcotics and other dangerous controlled substances, and their proceeds or instrumentalities from the sale of the controlled substances. Based on my training and experience, I also know that drug traffickers frequently use Priority Mail with delivery

confirmation, a two-three day service offered by the United States Postal Service. As a result of investigations and successful controlled substance prosecutions where the U.S. Mail was used, I have learned of certain characteristics indicative of other U.S Mail items previously identified as containing narcotics or other dangerous controlled substances, their proceeds or instrumentalities from the sale of the controlled substances. Some of these characteristics include, but are not necessarily limited to or used on every occasion, the mailer using different post offices on the same day to send parcels, false or non-existent return address, the addressee is not known to receive mail at the listed delivery address, the parcel is heavily taped, the parcel is mailed from a known drug source location, labeling information contains misspellings, the label contains an illegible waiver signature, unusual odors emanating from the parcel, and the listed address is located in an area of known or suspected drug activity.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

A. USPIS intercepted a package containing approximately two kilograms of a white pressed powder that field-tested positive for fentanyl, a Schedule II controlled substance.

5. On January 20, 2023, the U.S. Postal Inspection Service intercepted a USPS Priority Mail Express Large Flat Rate box, bearing tracking number 9505 5128 5962 3018 6397 28 (the "SUBJECT PACKAGE") at the Dayton Processing and Distribution Center in Dayton, OH. The SUBJECT PACKAGE is a USPS Priority Mail Express Large Flat Rate box, bearing tracking number 9505 5128 5962 3018 6397 28, mailed from Post Office 91761, located in the Los Angeles, California Metropolitan Area, postmarked January 18, 2023. I know, based on my training and experience, that California is a known source location for narcotics. The recipient's

information listed on the SUBJECT PACKAGE is "Uriel Garcia, 26 Andrews St., Dayton, OH 45410." The sender's information listed on the SUBJECT PACKAGE is "Fernando Rodriguez, 1305 E. 4th. St., Ontario, CA."

6. I performed a check in CLEAR for the recipient's information listed on the SUBJECT PACKAGE. CLEAR is a law enforcement database that is used as a tool for investigators to identify person/business and address information. According to CLEAR, there is no "Uriel Garcia" associated with 26 Andrews St., Dayton, OH 45410.

7. I also performed a check in CLEAR for the sender's information listed on the SUBJECT PACKAGE. According to CLEAR, there is no "Fernando Rodriguez" associated with 1305 E. 4th. St., Ontario, CA 91764.

8. A certified drug detection canine officer performed an open-air sniff on the SUBJECT PACKAGE and alerted to the presence of an odor of controlled substances emanating from the SUBJECT PACKAGE.

9. As a result of my investigation, on January 20, 2023, I obtained and executed a federal search warrant on the SUBJECT PACKAGE. Upon opening the SUBJECT PACKAGE, I discovered that it contained two separate packages wrapped with gift wrap. Inside the gift wrap was a "Fruit Loops" cereal box. Inside the cereal box was a padded yellow envelope. Inside the padded yellow envelope was several layers of black vacuum-sealed bags with dryer sheets. Inside the vacuum-sealed bags was a brown taped block/kilo of pressed white powder with "WILIAM" in marker written on it. The second gift-wrapped box contained the same pressed white powder block/kilo, which was packaged the same way. I know, based on my training and experience, and as I explain in further detail below, that drug traffickers frequently attempt to mask the odor of narcotics by using plastic wrap, vacuum-sealed bags, and dryer sheets to package the drugs.

10. The total approximate weight of the two blocks/kilos was 5.1 pounds or 2313.32 grams. One of the blocks/kilos was field-tested using a TRUNARC narcotics analyzer. The TRUNARC narcotics analyzer alerted positively to the presence of fentanyl, a Schedule II controlled substance. Based on my training and experience, the pressed white powder blocks/kilos are consistent in appearance with fentanyl. I will send the substance to a laboratory for forensic testing to confirm my belief that the pressed white powder is in fact fentanyl.

B. A USPS agent will attempt to deliver the SUBJECT PACKAGE to the PREMISES; if someone at the PREMISES accepts delivery of the SUBJECT PACKAGE, USPS agents will execute a search of the PREMISES.

11. Agents involved in this investigation are separately seeking a search warrant to place a GPS tracking device and a light detection device inside the SUBJECT PACKAGE. Agents will replace the suspected fentanyl with "sham" drugs and attempt delivery of the SUBJECT PACKAGE containing the sham drugs and tracking device at the PREMISES and then serve this search warrant. A United States Postal Inspector posing as a United States Letter Carrier will attempt to make contact with an occupant at the PREMISES. If and when a person at the PREMISES answers the door, the agent will ask the person to acknowledge receipt of the SUBJECT PACKAGE.

12. If no one is home when agents attempt to deliver the SUBJECT PACKAGE, agents will try again until the final date for which the Court authorizes execution of this search warrant. During all delivery attempts, law enforcement officers involved will maintain surveillance on the SUBJECT PACKAGE.

13. CONDITION PRECEDENT: This search warrant will only be served after the SUBJECT PACKAGE has been delivered to and received by someone at the PREMISES and taken into the PREMISES. At that time, and not before, I and other law enforcement personnel will execute this search warrant. In no event will the search warrant be executed if the SUBJECT PACKAGE is not taken into the PREMISES.

14. Further, if the SUBJECT PACKAGE is transferred to any vehicle or other property located within this Court's jurisdiction, this order authorizes law enforcement to secure the location until an application for a new warrant can be obtained.

BACKGROUND ON DRUG TRAFFICKERS

15. Based on my training and experience, I know that the following are common practices of drug traffickers, and that evidence of these common practices is likely to be found at any premises and/or electronic devices (such as cell phones) used by drug traffickers:

i. Drug dealers commonly store drugs and drug paraphernalia, including pipes, syringes, and rolling papers, in their residences, stash houses, and/or vehicles in order to have ready access to the drugs and/or paraphernalia in order to conduct their drug dealing business or to use those drugs personally;

ii. Drug dealers attempt to mask the distinct odors of particular drugs through the use of heat sealing and/or canning devices and/or aromatic substances such as laundry soap, dryer sheets, air fresheners, or axle grease;

iii. Drug dealers often dilute, or "cut," drugs in order to maximize the volume of drugs they have to sell, and thus their profits. Drug dealers use various substances to dilute drugs, including mannitol, mannite, lactose, Vitamin B12, and MSM. Drug dealers use equipment, such as scales, sifters, hammers, grinders, razor blades, glass panes, mirrors and kilo or pound presses as part of the dilution or "cutting" process. Once the drug has been "cut," drug dealers usually will repackage it, often in smaller quantities, using masking agents, tape, heat sealers and heat sealed bags, ziplocs bags, paper bindles, and/or other containers for redistribution. It is common for drug dealers to maintain such equipment and supplies in their residences and stash houses;

iv. Drug dealers keep books, receipts, notes, ledgers and other forms of records specifically relating to their drug distribution activities. Because drug dealers often "front" drugs to their customers – that is, sell the drugs on credit – or receive drugs from their suppliers on credit, such documentation is necessary to keep track of the amounts paid and owed with respect to their customers and suppliers. These ledgers are more commonly known as "pay/owe sheets" and may be as simple as notations on miscellaneous

pieces of paper or may be recorded more formally in notebooks or even computer spreadsheets, and are frequently encoded in order to protect those involved. Drug dealers often keep such records on their person or in their residences, stash houses, and/or vehicles;

v. Drug dealing is a cash business. Customers pay for drugs with cash and dealers commonly purchase drugs from their suppliers with cash. Drug dealers commonly keep large sums of currency, financial instruments, precious metals, jewelry, and other items of value which represent either the proceeds from drug sales or are intended for the purchase of controlled substances. When drug dealers amass such wealth, they often attempt to legitimize that wealth or otherwise conceal it and its origin from discovery by law enforcement. To accomplish this, drug dealers often use different techniques, including the use of foreign and domestic banks and their attendant services, including savings and checking accounts, securities, cashier's checks, money drafts and letters of credit to exchange drug proceeds into money that appears to come from a legitimate source. Drug dealers also purchase real estate or vehicles, and establish shell corporations and business fronts that they use to launder drug proceeds. Drug dealers often utilize fictitious or "straw-holder" owners to conceal the true ownership, vehicles, or other valuable items purchased with the proceeds of illicit drug sales. In addition, drug dealers often use wire transfers, cashier's checks, and money orders to pay for drugs or other costs relating to their distribution business. Drug dealers often keep these items of value, and records relating to them, on their person or in their residences, stash houses, and/or vehicles where they are concealed from law enforcement and readily available.

vi. Drug dealers go to great lengths to hide and secure the drugs, drug proceeds, other items of value and records relating to their drug business. This is to safeguard those items against robbery and keep them from law enforcement. These secure locations typically include safes, vaults, or other locked containers, as well as specially constructed concealed compartments such as those often found in vehicles used specifically to facilitate drug dealing. Other methods of concealment include the burial of such items underground, the use of locked vehicles, trailers, out buildings, sheds, and/or exterior closets, the use of natural spaces within walls, furniture, vehicles, and other areas, and the use of sealed cans and canning machines;

vii. Drug dealers often use the United States Postal Service or commercial express mail delivery companies, such as FedEx or UPS, to ship drugs and money to various points within the United States. They do so, at least in

part, due to the convenience of the service and the availability of related internet and phone tracking services, speed of delivery, and to reduce their risk of arrest during the transportation of drugs from one place to another. They often use hand-written airbills, drop the packages near closing time, pay for such services in cash and utilize false or nominee names, addresses, and/or telephone numbers when using such services in order to further insulate themselves from detection by law enforcement. Drug dealers frequently maintain records relating to their use of these services, such as receipts, copies of airbills, empty and/or previously used boxes, packing tape, packing popcorn/filler and other packaging materials, and package tracking records printed from the internet, at their residences, stash houses, and/or in their vehicles where they are available for reference.

viii. Drug dealing is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package and deliver the drugs and persons to launder the drug proceeds. These persons frequently maintain listings of names, aliases, telephone numbers, pager numbers, facsimile numbers, physical addresses, and email addresses, sometimes encoded and sometimes not encoded, for the purpose of contacting their suppliers, customers, transporters, and others involved in their illicit drug distribution activities. These records are typically maintained on their person or in their residences, stash houses, and/or vehicles, so they are readily available in order to efficiently conduct their drug dealing business. Moreover, such records are often stored electronically within the memory of telephones, computers, and/or personal digital assistants such as iPhone and Blackberry devices;

ix. Drug dealers often use cellular telephones, satellite telephones, pagers and text messaging devices, voicemail or answering machine systems, telephone calling cards, computers, email, and/or personal digital assistants such as iPhone and Blackberry devices in order to communicate with their suppliers, customers, transporters, and others involved in their illicit drug distribution activities. Drug dealers often keep these items on their person or in their residences, stash houses, businesses, and/or vehicles where they are readily available;

x. Drug dealers often travel by car, bus, train, or airplane, both domestically and to and/or within foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, or to transport drugs or drug proceeds. Documents relating to such travel, such as calendars, travel itineraries, maps, airline ticket and baggage stubs, frequent use club membership information and records associated with

airlines, rental car companies, and/or hotels, airline, hotel and rental car receipts, credit card bills and receipts, photographs, videos, passports, and visas, are often maintained by drug dealers in their residences, stash houses, and/or vehicles where they are readily available for use or reference;

xi. Drug dealers frequently possess firearms, ammunition, silencers, explosives, incendiary devices, and other dangerous weapons to protect their profits, supply of drugs, and persons from others who might attempt to forcibly take such items and/or harm them during transactions. Such weapons, which are often stolen or otherwise possessed illegally, are typically maintained on their person or in their residences, stash houses, and/or vehicles where they are concealed from law enforcement and readily available;

xii. Drug dealers frequently take, or cause to be taken, photographs and/or videos of themselves, their criminal associates, their real and personal property, their weapons, and their drugs; and such items are often stored on their person, in their residences, and/or vehicles;

xiii. During the course of a search it is not uncommon to find items of personal property that tend to identify the person(s) in residence occupancy, control, or ownership of the place being searched vehicle, such as cancelled mail, deeds, leases, titles, registration information, rental agreements, photographs, videos, diaries, utility and telephone bills, tax documentation, travel documents, statements, passports, driver's licenses and/or identification cards, immigration documentation, birth certificates, and keys;

xiv. Drug dealers often utilize two-way radios, police scanners, video surveillance systems, and other counter surveillance equipment to prevent detection by law enforcement, and that such items are typically maintained at their residences, stash houses, and/or in their vehicles; and

xv. I know that drug dealers often use their vehicles to transport contraband – including drugs, drug proceeds and firearms – and other evidence of their activities. I know that following a drug trafficker's movements can facilitate surveillance and enable agents to follow a subject without exposing themselves to the subject they are following. This in turn enables agents to observe a drug trafficker's meetings with other associates and learn about new locations where a DTO stores drugs, money, firearms and other items related to the manufacture and distribution of controlled substances.

TECHNICAL TERMS

16. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

17. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

18. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or

years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes

19. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how

computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information,

communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a

digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

20. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the

warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

22. Because several people may share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

23. Based upon the facts set forth in this Affidavit, there is probable cause to believe that, if the SUBJECT PACKAGE is delivered and taken into the residence at the PREMISES, the items described in Attachment B exist and can be found at the PREMISES.

//

//

//

//

//

//

//

//

//

REQUEST FOR SEALING

24. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Sean C. Humphrey

Sean C. Humphrey
Task Force Officer
United States Postal Inspection Service

Subscribed and sworn to before me on January 23, 2023.
By reliable electronic means (telephone)

Caroline H. Gentry
United States Magistrate Judge

ATTACHMENT A

Property to be searched

The property to be searched, pictured below, is 26 Andrews St., Dayton, OH 45410, including all outbuildings and curtilage, further described as the right/west half of a duplex-style home with yellow siding and white trim. The number "26" is in white on the white pillar to the right of the front door.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 21 U.S.C. §§ 846, 843, and 841(a)(1), those violations involving unknown suspects and occurring after January 1, 2023, including:

a. Log books, records, payment receipts, notes, and/or customer lists, ledgers, telephone numbers and other papers or electronic records relating to the transportation, ordering, purchasing, processing, and distribution of controlled substances, including information reflecting transactions for the purchase/sale of narcotics.

b. Papers, tickets, notices, credit card receipts, wire transfer receipts, travel schedules, travel receipts, passports, and/or records, and other items relating to domestic and foreign travel to obtain and distribute narcotics and narcotics proceeds, including, but not limited to airline receipts, vehicle rental receipts, credit card receipts, travel schedules, diaries, hotel receipts, truck logs, travel agency vouchers, notes, records of long distance telephone calls, e-mail, calendars and other correspondence.

c. Address and/or telephone books and papers reflecting names, e-mail and physical addresses and/or telephone numbers of individuals, partnerships, or corporations involved in drug trafficking and money laundering.

d. Financial records, financial statements, receipts, statements of accounts and related bank records, money, drafts, letters of credit, money orders and cashier's checks receipts, passbooks, bank checks, escrow documents, and other items evidencing the obtaining, secreting, transfer, and/or concealment of assets and the obtaining, secreting, transferring, concealment, and/or expenditure of money.

e. Electronic equipment such as pagers, computers, Computer systems, cell phones, PDA devices including hardware, software, data contained in the main unit, printers, external modems, monitors, fax machines and/or other external attachments, electronic organizers, facsimile machines, cellular telephones, caller ID, telephone answering machines, police scanners and two-way radios.

f. United States currency, precious metals, coins, bullion, jewelry, and financial instruments, including, but not limited to stocks and bonds.

g. Photographs and/or photographic albums or video tapes and recordings of houses and other real estate, automobiles, and of other assets, persons, and/or controlled substances.

h. Indicia of occupancy, residency, and/or ownership of the premises and vehicles including, but not limited to utility and telephone bills, canceled envelopes, keys, deeds, tax bills, titles, and vehicle registrations.

i. Contraband, such as controlled substances and other materials, paraphernalia and/or equipment and tools used in the drug trade.

j. Firearms or ammunition.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

ATTACHMENT C

Upon delivery of the SUBJECT PACKAGE (as described in the Affidavit submitted with the warrant application) and the SUBJECT PACKAGE taken into the residence at the PREMISES, the search warrant will be executed at the PREMISES. The search warrant will be executed at the PREMISES if, and only if, the SUBJECT PACKAGE is taken into the residence located at the PREMISES.

Furthermore, if the SUBJECT PACKAGE is transferred to any vehicle or other property located within this Court's jurisdiction, this warrant authorizes law enforcement to secure the location until an application for a new warrant can be obtained.